FORM PTO-1390
(REV. 5-93)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
2345/165

JC10 Rec'd PCT/PTO 0 1 OCT 2001

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/937923

INTERNATIONAL APPLICATION NO	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED:
PCT/EP00/02481	**21 March 2000 (21.03.00)**	**30 March 1999 (30.03.99)**

TITLE
METHOD FOR GENERATING IDENTIFICATION NUMBERS

APPLICANT(S) FOR DO/EO/US
Joerg SCHWENK; Tobias MARTIN

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). (UNSIGNED)
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification and a marked up version of the substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report; International Preliminary Examination Report; and Form PCT/RO/101.

Express Mail No.: EL244508211US

U.S. APPLICATION NO if known, see 37 C.F.R. 1.5	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/937923	PCT/EP00/02481	2345/165

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Search Report has been prepared by the EPO or JPO $890.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) $710.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $740.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1,040.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 890	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	18 - 20 =	0	X $18.00	$0	
Independent Claims	1 - 3 =	0	X $84.00	$0	
Multiple dependent claim(s) (if applicable)			+ $280.00	$	
TOTAL OF ABOVE CALCULATIONS =				$890	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$890	
Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$890	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$890	
				Amount to be refunded	$
				charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $890.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
Kenyon & Kenyon
One Broadway
New York, New York 10004
Telephone No. (212)425-7200
Facsimile No. (212)425-5288

SIGNATURE

Richard L. Mayer, Reg. No. 22,490
NAME

10/1/2001
DATE

Reg. No. 33,865
Agent C
DE0157H

CUSTOMER NO. 26646

[2345/165]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Joerg SCHWENK et al.
Serial No.	:	To Be Assigned
Filed	:	Herewith
For	:	METHOD FOR GENERATING IDENTIFICATION NUMBERS
Art Unit	:	To Be Assigned
Examiner	:	To Be Assigned

Assistant Commissioner
for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT AND
37 C.F.R. § 1.125 SUBSTITUTE SPECIFICATION STATEMENT

SIR:

Please amend without prejudice the above-identified application before examination, as set forth below.

IN THE TITLE:

Please replace the title with the following:

--METHOD FOR GENERATING IDENTIFICATION NUMBERS--.

IN THE SPECIFICATION AND ABSTRACT:

In accordance with 37 C.F.R. § 1.121(b)(3), a Substitute Specification (including the Abstract, but without claims) accompanies this response. It is respectfully requested that the Substitute Specification (including Abstract) be entered to replace the Specification of record.

Express Mail No. EL 244508211 US

IN THE CLAIMS:

Without prejudice, please cancel original claims 1 to 17 in the original application, and please add new claims 18 to 35 as follows:

18. (New) A method for generating a personal identification number (PIN) having a number of N decimal digits, to be used for money cards and other security-requiring devices, comprising:

generating the personal identification number from a binary number having L digits so that the personal identification number is randomly distributed over an available number domain.

19. (New) The method of claim 18, further comprising:

converting a first predefinable natural number n1 of digits of the binary number into a decimal number d1;

wherein:

the first predefinable natural number n1 of digits is selected so as to yield a natural number z1 such that a quotient $2^{n1}/(z1*9)$ is close to 1;

a first decimal digit of the personal identification number receives a value d1 modulo 9; and

N-1 further groups of a predefinable number n2 of digits of the binary number are converted each time into N-1 decimal numbers d2 through dN, the predefinable number n2 being selected so as to yield a natural number z2 such that a quotient $2^{n2}/(z2*10)$ is close to 1, to satisfy a condition of $0<=2^{n2}$ modulo 10<3, and decimal digits 2 through N of the personal identification number receive values di modulo 10, i=2 through N.

20. (New) The method of claim 18, wherein n1 and n2<=16 are predefined.

21. (New) The method of claim 18, wherein N=4 is selected.

22. (New) The method of claim 18, wherein the binary number has a length of L=16, and N=4 and n1=n2=4 are predefined.

23. (New) The method of claim 18, wherein the binary number has a length L=3*n3, n3 groups of three digits of the binary number are converted into n3 decimal digits to generate n3 digits of the personal identification number, and n3 is a natural number.

24. (New) The method of claim 18, wherein the binary number is fully converted into a decimal number to generate the personal identification number, and if necessary, a correction value is added to a resultant decimal number so that a first digit of the decimal number becomes unequal to zero, digits of the resultant decimal number forming the decimal digits of the personal identification number.

25. (New) The method of claim 24, wherein the binary number has a length L of 13, the resultant decimal number has four digits, and a preset value greater than 999 and smaller than 1807 is added to the resultant decimal number.

26. (New) The method of claim 25, wherein a set of numbers 0 through 8191 is allocated to n5 subsets Ml, . . . , Mn5, and a preset value di is added to the resultant decimal number if it is an element of the set Mi, where 999<d1<d2< . . . <dn5<1809 and n5 is a natural number.

27. (New) The method of claim 24, wherein the binary number has a length L of 16, the resultant decimal number has five digits, and a preset value greater than 9999 and smaller than 34465 is added to the resultant decimal number.

28. (New) The method of claim 27, wherein a set of numbers 0 through 65535 is allocated to n5 subsets Ml, . . . , Mn5, and a preset value di is added to the resultant decimal number if it is an element of the set Mi, where 9999<d1<d2< . . . <dn5<34465 and n5 is a natural number.

29. (New) The method of claim 18, wherein:

a first digit of the personal identification number is generated by:

generating a pseudo-random number composed of up to 36 hexadecimal digits from a binary number of a length L;

converting each hexadecimal digit of the pseudo-random number using one different one out of 36 possible different mathematical mappings of the 36 hexadecimal digits into digits 1 through 9, into another digit of the digits 1 through 9, forming a generated number;

linking up to 36 decimal digits of a generated number in a mathematical operating to form a decimal digit that is unequal to zero and that represents a first digit of the personal identification number, to average out a probability of a particular personal identification digit occurring; and

a second digit and each following digit of the personal identification number is generated by:

generating another pseudo-random number composed of up to 210 hexadecimal digits from the binary number of length L;

converting each hexadecimal digit of the another pseudo-random number into one decimal digit using each time one different one out of a 210 possible mathematical mappings of hexadecimal digits into decimal digits; and

linking up to 210 decimal digits of a generated number in a mathematical operation to form a decimal digit representing a particular digit of the personal identification number, to average out the probability of the particular personal identification digit occurring.

30. (New) The method of claim 29, wherein the first digit of the personal identification number is generated in that the up to 36 digits are linked using a group operation of any arbitrary mathematical group of an order 9, and the second digit and each following digit of the personal identification number are generated in that the up to 210 digits are linked using a group operation of any arbitrary mathematical group of an order 10.

31. (New) The method of claim 30, wherein an additive group of integers modulo 10 are used to link the up to 210 digits.

32. (New) The method of claim 30, wherein a multiplicative group of integers modulo 11 are used to link the up to 210 digits.

33. (New) The method of claim 30, wherein a group of symmetric mappings of at least one of a regular pentagon and a dihedral group is used to link the up to 210 digits, each ten symmetric mappings of the group of symmetric mappings of the at least one of the regular pentagon and the dihedral group being assigned a different decimal digit.

34. (New) The method of claim 33, wherein a digit 0 is assigned to an identity mapping,

digits 1 through 4 are assigned to four rotations about a midpoint of the at least one of the regular pentagon and the dihedral group, and digits 5 through 9 are assigned to five reflections about five axes of symmetry of the at least one of the regular pentagon and the dihedral group.

35. The method of claim 18, wherein the binary number is a binary code specific to an individual.

REMARKS

This Preliminary Amendment cancels without prejudice original claims 1 to 17 in the underlying PCT Application No. PCT/EP00/02481, and adds without prejudice new claims 18 to 35. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

In accordance with 37 C.F.R. § 1.121(b)(3), the Substitute Specification (including the Abstract, but without the claims) contains no new matter. The amendments reflected in the Substitute Specification (including Abstract) are to conform the Specification and Abstract to U.S. Patent and Trademark Office rules or to correct informalities. As required by 37 C.F.R. § 1.121(b)(3)(iii) and § 1.125(b)(2), a Marked Up Version Of The Substitute Specification comparing the Specification of record and the Substitute Specification also accompanies this Preliminary Amendment. In the Marked Up Version, double-underlining indicates added text and bracketing indicates deleted text. Approval and entry of the Substitute Specification (including Abstract) is respectfully requested.

The underlying PCT Application No. PCT/EP00/02481 includes an International Search Report, dated August 30, 2000. The Search Report includes a list of documents that were uncovered in the underlying PCT Application. A copy of the Search Report accompanies this Preliminary Amendment.

The underlying PCT Application No. PCT/EP00/02481 also includes an International Preliminary Examination Report, dated February 26, 2001, and an annex associated with the International Preliminary Examination Report. An English translation of the International Preliminary Examination Report and of the annex accompanies this Preliminary Amendment.

Applicants assert that the subject matter of the present application is new, non-obvious, and useful. Prompt consideration and allowance of the application are respectfully requested.

Respectfully Submitted,

KENYON & KENYON

Dated: 10/1/2001

By: Richard Mayer (By Reg. No. 33,585 Aaron C Decker)

Richard L. Mayer
(Reg. No. 22,490)

One Broadway
New York, NY 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)

CUSTOMER NO. 26646

METHOD FOR GENERATING IDENTIFICATION NUMBERS

FIELD OF THE INVENTION

The present invention relates to a method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual.

BACKGROUND INFORMATION

When using automatic cash dispensers, such as ATM machines or similar devices where a plastic card is utilized, the user must often use a four-digit number (PIN) known only to himself in order to receive authorization. There are, by far, however, not as many different PINs as there are users, which is why each PIN exists many times over.

The PINs may only contain decimal digits, to enable them to be entered using numerical keypads. In addition, they are not supposed to begin with a zero. This means that, given four digit positions, the result is a range of 9000 different PINS. The theoretically lowest probability of correctly guessing a PIN is, thus, 1/9000.

SUMMARY OF THE INVENTION

An exemplary method and/or exemplary embodiment of the present invention is directed to providing a method which will keep the probability of a PIN being correctly guessed as low as possible.

When the PINs are generated such that they are randomly uniformly distributed over the available number domain, the probability of a PIN being correctly ascertained may then become minimal.

With the aid of an encryption algorithm, a secret key may be used to produce a binary code from personal data pertaining to the user. Using the DES (data encryption standard) or triple DES algorithm provided, for example, for generating PINs for money cards, a 64-digit binary code is generated from the data pertaining to one customer, with the assistance of a bank-specific key. From a 16-digit segment of this binary code, the PIN can be generated in the following manner.

For example, four parts for each of the four digits of this binary number are combined into four decimal numbers. These four decimal numbers are divided by 10 (modulo function) to yield the four digits of the PIN as a remainder of a division. If the first digit is a zero, it is replaced by a one. To a large degree, however, the resultant PINs are unevenly distributed over the available number domain of 1 to 9000. If it begins with a 1, a PIN generated in this manner has a probability of being correctly guessed of even greater than 1/150.

If, on the other hand, the PINs are distributed uniformly over the number domain, then the rate of occurrence of each PIN is constantly 1/9000, and the probability of it being correctly guessed is, therefore, also minimal.

Another exemplary embodiment and/or exemplary method of the present invention provides for the first nl digits of the binary number (B) to be converted in an available manner into a decimal number dl, the predefinable natural number nl being selected so as to yield a natural number z1 such that the quotient $2^{n1}/(z1*9)$ is close to 1; and for the first decimal digit of the PIN to receive the value dl modulo 9; for N-1 further groups of further n2 digits of the binary number (B) to be converted each time in an available manner into N-1 decimal numbers d2 through dN, the predefinable number n2 being selected so as to yield a natural number z2 such that

the quotient $2^{n2}/(z2*10)$ is close to 1, to satisfy the condition: $0<=2^{n2}$ modulo 10<3; and for the decimal digits 2 through N of the PIN to receive the values di modulo 10, i=2 through N.

To generate the first digit of the PIN, nl is selected so that 2^{n1} is close to a multiple of 9. The n-1 digit part to the front of the binary number is interpreted as a decimal number. The integer remainder is calculated by dividing by 9. This remainder forms the first digit of the PIN. To generate digit 2 and the following digits of the PIN, n2 bits are split off each time. The number n2 is selected such that 2^n is close to a multiple of 10. The resulting number is interpreted as a decimal number. The integer remainder is calculated by dividing by 10. This remainder forms the respective digit of the PIN. It is true that no absolute uniform distribution is derived hereby. However, the greater n2 is, the more uniformly the PIN numbers are distributed.

For example, selecting n2=13 results in a number domain of from 1 to 2^{13}=8192. The digits 0, 1, 2 and 3 occur in the generated PINs with a probability of 820/8192, and the remaining digits with a probability of 819/8192. The exemplary embodiments and/or exemplary methods of the present invention may avoid having the 1 occur all too often in the first digit position of the PIN.

A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for nl and n2<=16 to be predefined.

A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for N=4 to be selected.

A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for the binary

number (B) to have the length L=16, for N=4 to be predefined, and for n1=n2=4 to be predefined.

A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for the binary number (B) to have the length L=3*n3, for n3 groups of three digits of the binary number (B) to be converted in an available manner into n3 decimal digits to generate the digits of the PIN, n3 being a natural number. In this variant, altogether 12 bits of the customer-specific binary code are used to generate the PIN. In each case, three bits of this binary number are interpreted as decimal digits between 1 and 8. The PINs produced in this manner are absolutely uniformly distributed.

Another exemplary embodiment and/or exemplary method for generating absolutely uniformly distributed PINs within the particular number domain provides for the binary number to be completely converted into a decimal number, in order to generate the PIN in an available manner, and, if necessary, to add a correction value to the resultant decimal number such that the first digit of the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.

To this end, it may be provided for the binary number to have a length L of 13, for the generated decimal number to have four digits, and for a preset value greater than 999 and smaller than 1807 to be added to the decimal number; for the binary number to have a length L of 16, for the generated decimal number to have five digit positions, and for a preset value greater than 9999 and smaller than 34465 to be added to the decimal number.

Furthermore, it may be provided in the first case (L=13) for the set of numbers 0 through 8191 to be allocated to n5 subsets M1,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set

Mi, it holding that 999<dl<d2<...<dn5<1809, and n5 being a natural number.

Furthermore, it may be provided in the second case (L=16) for the set of numbers 0 through 65535 to be allocated to n5 subsets Ml,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set Mi, it holding that 9999<dl<d2<...<dn5<34465, and n5 being a natural number.

Another exemplary embodiment and/or exemplary method of the present invention provides for executing the following steps to generate the first digits of the PIN:

- a pseudo-random number composed of up to 36 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted using one different one out of the 36 possible mathematical mappings of hexadecimal digits into the digits 1 through 9, into a digit of the digits 1 through 9;
- to even out the probability of the particular PIN digit occurring, the up to 36 decimal digits of the thus generated number are linked or associated in a mathematical operation to form a decimal digit unequal to zero, which represents the first digit of the PIN;

and for the following steps to be executed for the second and each following digit of the PIN to be generated:

- .a pseudo-random number composed of up to 210 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted into one decimal digit using each time one different one out of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;
- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN;

In another exemplary embodiment and/or exemplary method, the first digit of the PIN may be generated so that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and that the second and the following digits of the PIN are generated, so that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.

In this exemplary embodiment and/or exemplary method of the present invention, one hexidecimal number each is generated from N groups of 4 bit length each. It is intended at this point to convert it into a decimal digit. Altogether (10 over 6) = (10 over 4) = 210 different mappings of the hexadecimal digits into the set of decimal digits are available for this conversion. One possible mapping is forming the remainder in a division operation by 10: (0 -> 0, 1 -> 1, 2 -> 2, 3 -> 3, 4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Following this mapping operation, the digits 0 to 5 occur with the rate of occurrence of 1/8, and the digits from 6 to 9 with the rate of occurrence of 1/16. At this point, in order to obtain digits whose probability of occurrence does not deviate or deviates imperceptibly from 1/10, it is proposed to convert the 210 hexadecimal digits, which were generated, for example, by applying the above-mentioned DES algorithm 14 times to the 64-digit binary initial number, (therefore, pseudo-random number, since the generated number is in no way randomly formed), using one each of the other 210 possible mappings, into a decimal digit and, subsequently, linking all 210 decimal digits to one single digit using a group operation of a mathematical group having ten elements. The probability of occurrence of each of the thus generated decimal digits is close to 1/10.

Another exemplary embodiment and/or exemplary method of the present invention is directed to providing for the additive

group of the integers modulo 10 to be used to link the up to 210 digits. In this context, 210 decimal digits are linked to form one single digit, in that one adds all digits and takes as a result, the remainder of a division of the sum by 10. The ten possible results that occur in the process constitute the elements of the additive group $Z_{10,+}$.

Another exemplary embodiment and/or exemplary method of the present invention provides for using the multiplicative group of the integers modulo 11 for linking the up to 210 digits. This group Z^*_{11} likewise has ten elements and is, therefore, suited for linking the numbers to a decimal digit. In Z^*_{11}, one calculates by multiplying two elements and dividing the result by 11. The remaining remainder forms the result of the operation. The zero is removed from the group. The 0 occurring in the digits indexes element no. 10 of the group Z^*_{11}.

Another exemplary embodiment and/or exemplary method of the present invention is directed to providing that the group of the symmetric mappings of a regular pentagon (dihedral group) be used for linking the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit. To this end, it may also be provided for the digit 0 to be assigned to the identity mapping, digits 1 through 4 to be assigned the four rotations about the midpoint of the pentagon, digits 5 through 9 to be assigned to the five reflections about the five axes of symmetry of the pentagon. If one executes two symmetric mappings one after another, then a symmetric mapping again results. Based on these allocations, one can set up the following multiplication table:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1

6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0.

With the assistance of this table, the 210 digits are linked to one single digit in that, utilizing the result from the previous operation as a row indicator and utilizing the next digit as a column indicator, the next result in the table is read off successively until all digits are considered. The last result forms the desired digit of the PIN.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a diagram for generating a customer-specific binary code.

Figure 2 shows a diagram for generating a PIN through conversion to a decimal number.

Figure 3 shows a diagram for generating a PIN by a digit-by-digit conversion into decimal numbers.

Figure 4 shows a diagram for generating a PIN by a digit-by-digit conversion, including modulus formation.

Figure 5 shows a diagram for generating a PIN by reducing hexadecimal numbers with the assistance of mathematical groups.

DETAILED DESCRIPTION

Figure 1 depicts a flow diagram for converting personal data Dc of a customer using a secret key K into a binary number B of L bits length. The binary number B is part of the 64-bit long encryption result, which was generated from the customer data Dc using the DES algorithm.

If the length of the binary number B equals 13, and if the number of the PIN digits to be generated equals 4, then the

PIN, as shown in Figure 2, can be generated by interpreting the binary number B as decimal number D by adding a constant C thereto. The constant is to be selected such that the PIN does not have any leading zeros. In this manner, 8192 different PINS can be generated, which are absolutely uniformly distributed over the number domain in question.

Figure 3 depicts how a binary number of length 13 can be converted into a PIN in that for each digit of the PIN to be generated, a number of bits of the binary number is converted into a decimal number, and a constant C is added to the resultant number D, to avoid having leading zeros of the PIN. In this manner, 7777 different PINS may be generated, which are absolutely uniformly distributed over the number domain in question.

Another example for generating nearly equally distributed PINs from a binary number B is illustrated in Figure 4. The binary number B has 52 digit positions. To generate the four-digit PIN, the binary number B is subdivided into four subsets, which, in the example, have the same length. Each of these subsets is interpreted as a decimal number. The first digit of the PIN is derived as a remainder of a division of the first decimal number by 9. The following digits of the PIN are derived in each case as a remainder of a division of the following decimal number by 10. In this manner, 9000 different PINS may be generated, which are absolutely uniformly distributed.

From the personal data Dc of a customer, as shown in Figure 5, a sequence of 210 hexadecimal digits is generated with the assistance of a secret key and a random-number generator, in that, for example, an encryption result of the DES algorithm from Figure 1 is again encrypted using the algorithm, and so forth. The 14 64-digit binary codes resulting therefrom are converted into 14 hexadecimal numbers Hi, each having 16

digits. Lined up, this yields 224 hexadecimal digits, of which 210 enter into the generation of the PIN.

There are 210 different possibilities fi for mapping the set of 16 hexadecimal digits into the set of the 10 decimal digits. Therefore, each of the 210 hexadecimal digits is converted using a different one of these mappings into a decimal digit di. In order to produce a digit Zi of a PIN from the 210 decimal digits, they are successively linked using the group operation F of any arbitrary ten-element mathematical group; the last result is the sought after digit. Thus, the previously non-uniform, statistical distribution of the 210 decimal digits is evened out. The entire process is repeated for each of the digit positions Z2 through Z4 of the PIN.

Analogously for the first digit of the PIN, 36 hexadecimal digits are generated, which are mapped with every other one of the 36 possible mappings of the hexadecimal digits into the set of the digits 1 through 9, into a digit between 1 and 9. The 36 decimal digits are linked to the first digit of the PIN using the group operation of any arbitrary mathematical group of the order 9. This enables 9000 different PINs to be generated which are nearly uniformly distributed. In generating 10^5 PINs, the maximum non-uniformities amounted to about 1.5 percent. This does not significantly raise the probability of a PIN being accidentally correctly guessed as compared to the theoretical minimum value. Thus, the method functions very reliably.

All mathematical groups having ten elements are fundamentally suited for use with this method. Known representatives include the additive group of the integers modulo 10, $Z_{10,+}$, the multiplicative group of the integers modulo 11, Z^*_{11}, as well as the group of the symmetric mapping(s) of a regular pentagon D5, the so-called dihedral group. In the last instance, one decimal digit, which may be used for the calculation, is assigned to each of the individual elements of the group.

ABSTRACT OF THE DISCLOSURE

A method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual, the PINs are generated such that they are randomly uniformly distributed over the available number domain.

[ ]

METHOD FOR GENERATING IDENTIFICATION NUMBERS

FIELD OF THE INVENTION

The present invention [is directed]relates to a method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in[ ] particular from a binary code specific to an individual.

BACKGROUND INFORMATION

When using automatic cash dispensers, such as ATM machines or similar devices where a plastic card is utilized, the user must often use a four-digit number (PIN) known only to himself in order to receive authorization. There are, by far, however, not as many different PINs as there are users, which is why each PIN exists many times over.[ ]

The PINs may only contain decimal digits, to enable them to be entered using numerical keypads. In addition, they are not supposed to begin with a zero. This means that, given four digit positions, the result is a range of 9000 different PINS. The theoretically lowest probability of correctly guessing a PIN is, thus, 1/9000.

SUMMARY OF THE INVENTION

[The object]An exemplary method and/or exemplary embodiment of the present invention is directed to [provide]providing a method which will keep the probability of a PIN being correctly guessed as low as possible.[ ]

[The realization underlying the present invention is that w]When the PINs are generated such that they are randomly

uniformly distributed over the available number domain, the probability of a PIN being correctly ascertained may then become[s] minimal. [This is elucidated on the basis of the following example.]

With the aid of an encryption algorithm, a secret key may be used to produce a binary code from personal data pertaining to the user. Using the DES (data encryption standard) or triple DES algorithm provided, for example, for generating PINs for money cards, a 64-digit binary code is generated from the data pertaining to one customer, with the assistance of a bank-specific key. From a 16-digit segment of this binary code, the PIN can be generated in the following manner[, for].

For example[:

Four], four parts for each of the four digits of this binary number are combined into four decimal numbers. These four decimal numbers are divided by 10 (modulo function) to yield the four digits of the PIN as a remainder of a division. If the first digit is a zero, it is replaced by a one. To a large degree, however, the resultant PINs are unevenly distributed over the available number domain of 1 to 9000. If it begins with a 1, a PIN generated in this manner has a probability of being correctly guessed of even greater than 1/150.

If, on the other hand, [one distributes the PINs]the PINs are distributed uniformly over the number domain, then the rate of occurrence of each PIN is constantly 1/9000, and the probability of it being correctly guessed is, therefore, also minimal.

[A first]Another exemplary embodiment and/or exemplary method of the present invention provides for the first nl digits of the binary number (B) to be converted in [generally known fashion]an available manner into a decimal number dl, the

predefinable natural number n1 being selected so as to yield a natural number z1 such that the quotient $2^{n1}/(z1*9)$ is close to 1; and for the first decimal digit of the PIN to receive the value d1 modulo 9; for N-1 further groups of further n2 digits of the binary number (B) to be converted each time in [generally known fashion]an available manner into N-1 decimal numbers d2 through dN, the predefinable number n2 being selected so as to yield a natural number z2 such that the quotient $2^{n2}/(z2*10)$ is close to 1,[the intention being] to satisfy the condition: $0<=2^{n2}$ modulo 10<3; and for the decimal digits 2 through N of the PIN to receive the values di modulo 10, i=2 through N.

To generate the first digit of the PIN, n1 is selected so that 2^{n1} is close to a multiple of 9. The n-1 digit part to the front of the binary number is interpreted as a decimal number. The integer remainder is calculated by dividing by 9. This remainder forms the first digit of the PIN. To generate digit 2 and the following digits of the PIN, n2 bits are split off each time. The number n2 is selected such that 2^n is close to a multiple of 10. The resulting number is interpreted as a decimal number. The integer remainder is calculated by dividing by 10. This remainder forms the respective digit of the PIN. It is true that no absolute uniform distribution is derived hereby. However, the greater n2 is, the more uniformly the PIN numbers are distributed.

For example, selecting n2=13 results in a number domain of from 1 to 2^{13}=8192. The digits 0, 1, 2 and 3 occur in the generated PINs with a probability of 820/8192, and the remaining digits with a probability of 819/8192. [In particular, the]The exemplary embodiments and/or exemplary methods of the present invention may avoid[s] having the 1 occur all too often in the first digit position of the PIN.

A further exemplary embodiment and/or exemplary method of the present invention [provides]is directed to providing for nl and n2<=16 to be predefined.

[Yet another]A further exemplary embodiment and/or exemplary method of the present invention [provides]is directed to providing for N=4 to be selected.

[Furthermore, it may be provided]A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for the binary number (B) to have the length L=16, for N=4 to be predefined, and for nl=n2=4 to be predefined.

[Yet another]A further exemplary embodiment and/or exemplary method of the present invention [provides]is directed to providing for the binary number (B) to have the length L=3*n3, for n3 groups of three digits of the binary number (B) to be converted in [generally known fashion]an available manner into n3 decimal digits to generate the digits of the PIN, n3 being a natural number. In this variant, altogether 12 bits of the customer-specific binary code are used to generate the PIN. In each case, three bits of this binary number are interpreted as decimal digits between 1 and 8. The PINs produced in this manner are absolutely uniformly distributed.

Another [possibility]exemplary embodiment and/or exemplary method for generating absolutely uniformly distributed PINs within the particular number domain provides for the binary number to be completely converted into a decimal number, in order to generate the PIN in [generally known fashion]an available manner, and, if necessary, to add a correction value to the resultant decimal number such that the first digit of the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.

To this end, it may be provided for the binary number to have a length L of 13, for the generated decimal number to have four digits, and for a preset value greater than 999 and smaller than 1807 to be added to the decimal number; for the binary number to have a length L of 16, for the generated decimal number to have five digit positions, and for a preset value greater than 9999 and smaller than 34465 to be added to the decimal number.

Furthermore, it may be provided in the first case (L=13) for the set of numbers 0 through 8191 to be allocated to n5 subsets Ml,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set Mi, it holding that 999<dl<d2<...<dn5<1809, and n5 being a natural number.

Furthermore, it may be provided in the second case (L=16) for the set of numbers 0 through 65535 to be allocated to n5 subsets Ml,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set Mi, it holding that 9999<dl<d2<...<dn5<34465, and n5 being a natural number.

Another exemplary embodiment and/or exemplary method of the present invention provides for executing the following steps to generate the first digits of the PIN:

- a pseudo-random number composed of up to 36 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted using one different one out of the 36 possible mathematical mappings of hexadecimal digits into the digits 1 through 9, into a digit of the digits 1 through 9;
- to even out the probability of the particular PIN digit occurring, the up to 36 decimal digits of the thus generated number are linked or associated in a mathematical operation

to form a decimal digit unequal to zero, which represents the first digit of the PIN;

and for the following steps to be executed for the second and each following digit of the PIN to be generated:

- a pseudo-random number composed of up to 210 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted into one decimal digit using each time one different one out of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;
- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN;

[For this purpose]In another exemplary embodiment and/or exemplary method,[it may be provided that] the first digit of the PIN [is]may be generated [in]so that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and that the second and the following digits of the PIN are generated, [in]so that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.

In this exemplary embodiment [of the]and/or exemplary method of the present invention, one hexidecimal number each is generated from N groups of 4 bit length each. It is intended at this point to convert it into a decimal digit. Altogether (10 over 6) = (10 over 4) = 210 different mappings of the hexadecimal digits into the set of decimal digits are available for this conversion. One possible mapping is forming the remainder in a division operation by 10: (0 -> 0, 1 -> 1, 2 -> 2, 3 -> 3, 4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Following this mapping operation, the digits 0 to 5 occur with the rate

of occurrence of 1/8, and the digits from 6 to 9 with the rate of occurrence of 1/16. At this point, in order to obtain digits whose probability of occurrence does not deviate or deviates imperceptibly from 1/10, it is proposed to convert the 210 hexadecimal digits, which were generated, for example, by applying the above-mentioned DES algorithm 14 times to the 64-digit binary initial number, (therefore, pseudo-random number, since the generated number is in no way randomly formed), using one each of the other 210 possible mappings, into a decimal digit and, subsequently, linking all 210 decimal digits to one single digit using a group operation of a mathematical group having ten elements. The probability of occurrence of each of the thus generated decimal digits is close to 1/10.

[A next]Another exemplary embodiment and/or exemplary method of the present invention [provides]is directed to providing for the additive group of the integers modulo 10 to be used to link the up to 210 digits. In this context, 210 decimal digits are linked to form one single digit, in that one adds all digits and takes as a result, the remainder of a division of the sum by 10. The ten possible results that occur in the process constitute the elements of the additive group $Z_{10,+}$.

Another exemplary embodiment and/or exemplary method of the present invention provides for using the multiplicative group of the integers modulo 11 for linking the up to 210 digits. This group Z^*_{11} likewise has ten elements and is, therefore, suited for linking the numbers to a decimal digit. In Z^*_{11}, one calculates by multiplying two elements and dividing the result by 11. The remaining remainder forms the result of the operation. The zero is removed from the group. The 0 occurring in the digits indexes element no. 10 of the group Z^*_{11}.

Another exemplary embodiment and/or exemplary method of the present invention [provides]is directed to providing that the group of the symmetric mappings of a regular pentagon

(dihedral group) be used for linking the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit. To this end, it may also be provided for the digit 0 to be assigned to the identity mapping, digits 1 through 4 to be assigned the four rotations about the midpoint of the pentagon, digits 5 through 9 to be assigned to the five reflections about the five axes of symmetry of the pentagon. If one executes two symmetric mappings one after another, then a symmetric mapping again results. Based on these allocations, one can set up the following multiplication table:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0.

With the assistance of this table, the 210 digits are linked to one single digit in that, utilizing the result from the previous operation as a row indicator and utilizing the next digit as a column indicator, the next result in the table is read off successively until all digits are considered. The last result forms the desired digit of the PIN.

[Exemplary embodiments of the present invention are represented by several figures in the drawing and are elucidated in the following description. The figures show:

Figure 1]BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a diagram for generating a customer-specific binary code[;

].

Figure 2[ ] shows a diagram for generating a PIN through conversion to a decimal number[;].

Figure 3[ ] shows a diagram for generating a PIN by a digit-by-digit conversion into decimal numbers[;
].

Figure 4[ ] shows a diagram for generating a PIN by a digit-by-digit conversion, including modulus formation[; and
].

Figure 5[ ] shows a diagram for generating a PIN by reducing hexadecimal numbers with the assistance of mathematical groups.[
Identical or corresponding parts are provided with the same reference numerals in the figures.
]

DETAILED DESCRIPTION

Figure 1 depicts a flow diagram for converting personal data Dc of a customer using a secret key K into a binary number B of L bits length. The binary number B is part of the 64-bit long encryption result, which was generated from the customer data Dc using the DES algorithm.[
]

If the length of the binary number B equals 13, and if the number of the PIN digits to be generated equals 4, then the PIN, as shown in Figure 2, can be generated by interpreting the binary number B as decimal number D by adding a constant C thereto. The constant is to be selected such that the PIN does not have any leading zeros. In this manner, 8192 different PINS can be generated, which are absolutely uniformly distributed over the number domain in question.

Figure 3 depicts how a binary number of length 13 can be converted into a PIN in that for each digit of the PIN to be generated, a number of bits of the binary number is converted into a decimal number, and a constant C is added to the resultant number D, to avoid having leading zeros of the PIN. In this manner, 7777 different PINS may be generated, which are absolutely uniformly distributed over the number domain in question.

Another [possibility]example for generating nearly equally distributed PINs from a binary number B is illustrated in Figure 4. The binary number B has 52 digit positions. To generate the four-digit PIN, the binary number B is subdivided into four subsets, which, in the example, have the same length. Each of these subsets is interpreted as a decimal number. The first digit of the PIN is derived as a remainder of a division of the first decimal number by 9. The following digits of the PIN are derived in each case as a remainder of a division of the following decimal number by 10. In this manner, 9000 different PINS may be generated, which are absolutely uniformly distributed.

From the personal data Dc of a customer, as shown in Figure 5, a sequence of 210 hexadecimal digits is generated with the assistance of a secret key and a random-number generator, in that, for example, an encryption result of the DES algorithm from Figure 1 is again encrypted using the algorithm, and so forth. The 14 64-digit binary codes resulting therefrom are converted into 14 hexadecimal numbers Hi, each having 16 digits. Lined up, this yields 224 hexadecimal digits, of which 210 enter into the generation of the PIN.

There are 210 different possibilities fi for mapping the set of 16 hexadecimal digits into the set of the 10 decimal digits. Therefore, each of the 210 hexadecimal digits is converted using a different one of these mappings into a

decimal digit di. In order to produce a digit Zi of a PIN from the 210 decimal digits, they are successively linked using the group operation F of any arbitrary ten-element mathematical group; the last result is the sought after digit. Thus, the previously non-uniform, statistical distribution of the 210 decimal digits is evened out. The entire process is repeated for each of the digit positions Z2 through Z4 of the PIN.

Analogously for the first digit of the PIN, 36 hexadecimal digits are generated, which are mapped with every other one of the 36 possible mappings of the hexadecimal digits into the set of the digits 1 through 9, into a digit between 1 and 9. The 36 decimal digits are linked to the first digit of the PIN using the group operation of any arbitrary mathematical group of the order 9. This enables 9000 different PINs to be generated which are nearly uniformly distributed. In generating 10^5 PINs, the maximum non-uniformities amounted to about 1.5 percent. This does not significantly raise the probability of a PIN being accidentally correctly guessed as compared to the theoretical minimum value. Thus, the method functions very reliably.

All mathematical groups having ten elements are fundamentally suited for use with this method. Known representatives include the additive group of the integers modulo 10, $Z_{10,+}$, the multiplicative group of the integers modulo 11, Z^*_{11}, as well as the group of the symmetric [mappings]mapping(s) of a regular pentagon D5, the so-called dihedral group. In the last instance, one decimal digit, which may be used for the calculation, is assigned to each of the individual elements of the group.

[

Abstract

]

ABSTRACT OF THE DISCLOSURE

[In a]A method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual, the PINs are generated such that they are randomly uniformly distributed over the available number domain.

[2345/165]

METHOD FOR GENERATING IDENTIFICATION NUMBERS

The present invention is directed to a method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual.

When using automatic cash dispensers, such as ATM machines or similar devices where a plastic card is utilized, the user must often use a four-digit number (PIN) known only to himself in order to receive authorization. There are, by far, however, not as many different PINs as there are users, which is why each PIN exists many times over.

The PINs may only contain decimal digits, to enable them to be entered using numerical keypads. In addition, they are not supposed to begin with a zero. This means that, given four digit positions, the result is a range of 9000 different PINS. The theoretically lowest probability of correctly guessing a PIN is, thus, 1/9000.

The object of the present invention is to provide a method which will keep the probability of a PIN being correctly guessed as low as possible.

The realization underlying the present invention is that when the PINs are generated such that they are randomly uniformly distributed over the available number domain, the probability of a PIN being correctly ascertained becomes minimal. This is elucidated on the basis of the following example.

With the aid of an encryption algorithm, a secret key may be used to produce a binary code from personal data pertaining to the user. Using the DES or triple DES algorithm provided, for example, for generating PINs for money cards, a 64-digit

binary code is generated from the data pertaining to one customer, with the assistance of a bank-specific key. From a 16-digit segment of this binary code, the PIN can be generated in the following manner, for example:

Four parts for each of the four digits of this binary number are combined into four decimal numbers. These four decimal numbers are divided by 10 (modulo function) to yield the four digits of the PIN as a remainder of a division. If the first digit is a zero, it is replaced by a one. To a large degree, however, the resultant PINs are unevenly distributed over the available number domain of 1 to 9000. If it begins with a 1, a PIN generated in this manner has a probability of being correctly guessed of even greater than 1/150.

If, on the other hand, one distributes the PINs uniformly over the number domain, then the rate of occurrence of each PIN is constantly 1/9000, and the probability of it being correctly guessed is, therefore, also minimal.

A first exemplary embodiment of the present invention provides for the first nl digits of the binary number (B) to be converted in generally known fashion into a decimal number dl, the predefinable natural number nl being selected so as to yield a natural number z1 such that the quotient $2^{n1}/(z1*9)$ is close to 1; and for the first decimal digit of the PIN to receive the value dl modulo 9; for N-1 further groups of further n2 digits of the binary number (B) to be converted each time in generally known fashion into N-1 decimal numbers d2 through dN, the predefinable number n2 being selected so as to yield a natural number z2 such that the quotient $2^{n2}/(z2*10)$ is close to 1, the intention being to satisfy the condition: $0<=2^{n2}$ modulo 10<3; and for the decimal digits 2 through N of the PIN to receive the values di modulo 10, i=2 through N.

To generate the first digit of the PIN, nl is selected so that 2^{n1} is close to a multiple of 9. The n-1 digit part to the

front of the binary number is interpreted as a decimal number. The integer remainder is calculated by dividing by 9. This remainder forms the first digit of the PIN. To generate digit 2 and the following digits of the PIN, n2 bits are split off each time. The number n2 is selected such that 2^n is close to a multiple of 10. The resulting number is interpreted as a decimal number. The integer remainder is calculated by dividing by 10. This remainder forms the respective digit of the PIN. It is true that no absolute uniform distribution is derived hereby. However, the greater n2 is, the more uniformly the PIN numbers are distributed.

For example, selecting n2=13 results in a number domain of from 1 to 2^{13}=8192. The digits 0, 1, 2 and 3 occur in the generated PINs with a probability of 820/8192, and the remaining digits with a probability of 819/8192. In particular, the method of the present invention avoids having the 1 occur all too often in the first digit position of the PIN.

A further exemplary embodiment of the present invention provides for nl and n2<=16 to be predefined.

Yet another exemplary embodiment of the present invention provides for N=4 to be selected.

Furthermore, it may be provided for the binary number (B) to have the length L=16, for N=4 to be predefined, and for nl=n2=4 to be predefined.

Yet another exemplary embodiment of the present invention provides for the binary number (B) to have the length L=3*n3, for n3 groups of three digits of the binary number (B) to be converted in generally known fashion into n3 decimal digits to generate the digits of the PIN, n3 being a natural number. In this variant, altogether 12 bits of the customer-specific binary code are used to generate the PIN. In each case, three bits of this binary number are interpreted as decimal digits

between 1 and 8. The PINs produced in this manner are absolutely uniformly distributed.

Another possibility for generating absolutely uniformly distributed PINs within the particular number domain provides for the binary number to be completely converted into a decimal number, in order to generate the PIN in generally known fashion, and, if necessary, to add a correction value to the resultant decimal number such that the first digit of the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.

To this end, it may be provided for the binary number to have a length L of 13, for the generated decimal number to have four digits, and for a preset value greater than 999 and smaller than 1807 to be added to the decimal number; for the binary number to have a length L of 16, for the generated decimal number to have five digit positions, and for a preset value greater than 9999 and smaller than 34465 to be added to the decimal number.

Furthermore, it may be provided in the first case (L=13) for the set of numbers 0 through 8191 to be allocated to n5 subsets M1,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set Mi, it holding that 999<d1<d2<...<dn5<1809, and n5 being a natural number.

Furthermore, it may be provided in the second case (L=16) for the set of numbers 0 through 65535 to be allocated to n5 subsets M1,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set Mi, it holding that 9999<d1<d2<...<dn5<34465, and n5 being a natural number.

Another exemplary embodiment of the present invention provides for executing the following steps to generate the first digits of the PIN:

- a pseudo-random number composed of up to 36 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted using one different one out of the 36 possible mathematical mappings of hexadecimal digits into the digits 1 through 9, into a digit of the digits 1 through 9;
- to even out the probability of the particular PIN digit occurring, the up to 36 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit unequal to zero, which represents the first digit of the PIN;

and for the following steps to be executed for the second and each following digit of the PIN to be generated:

- a pseudo-random number composed of up to 210 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted into one decimal digit using each time one different one out of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;
- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN;

For this purpose, it may be provided that the first digit of the PIN is generated in that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and that the second and the following digits of the PIN are generated, in that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.

In this exemplary embodiment of the method of the present invention, one hexidecimal number each is generated from N groups of 4 bit length each. It is intended at this point to convert it into a decimal digit. Altogether (10 over 6) = (10

over 4) = 210 different mappings of the hexadecimal digits into the set of decimal digits are available for this conversion. One possible mapping is forming the remainder in a division by 10: (0 -> 0, 1 -> 1, 2 -> 2, 3 -> 3, 4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Following this mapping operation, the digits 0 to 5 occur with the rate of occurrence of 1/8, and the digits from 6 to 9 with the rate of occurrence of 1/16. At this point, in order to obtain digits whose probability of occurrence does not deviate or deviates imperceptibly from 1/10, it is proposed to convert the 210 hexadecimal digits, which were generated, for example, by applying the above-mentioned DES algorithm 14 times to the 64-digit binary initial number, (therefore, pseudo-random number, since the generated number is in no way randomly formed), using one each of the other 210 possible mappings, into a decimal digit and, subsequently, linking all 210 decimal digits to one single digit using a group operation of a mathematical group having ten elements. The probability of occurrence of each of the thus generated decimal digits is close to 1/10.

A next exemplary embodiment of the present invention provides for the additive group of the integers modulo 10 to be used to link the up to 210 digits. In this context, 210 decimal digits are linked to form one single digit, in that one adds all digits and takes as a result, the remainder of a division of the sum by 10. The ten possible results that occur in the process constitute the elements of the additive group $Z_{10,+}$.

Another exemplary embodiment of the present invention provides for using the multiplicative group of the integers modulo 11 for linking the up to 210 digits. This group Z^*_{11} likewise has ten elements and is, therefore, suited for linking the numbers to a decimal digit. In Z^*_{11}, one calculates by multiplying two elements and dividing the result by 11. The remaining remainder forms the result of the operation. The zero is

removed from the group. The 0 occurring in the digits indexes element no. 10 of the group Z^*_{11}.

Another exemplary embodiment of the present invention provides that the group of the symmetric mappings of a regular pentagon (dihedral group) be used for linking the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit. To this end, it may also be provided for the digit 0 to be assigned to the identity mapping, digits 1 through 4 to be assigned the four rotations about the midpoint of the pentagon, digits 5 through 9 to be assigned to the five reflections about the five axes of symmetry of the pentagon. If one executes two symmetric mappings one after another, then a symmetric mapping again results. Based on these allocations, one can set up the following multiplication table:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0.

With the assistance of this table, the 210 digits are linked to one single digit in that, utilizing the result from the previous operation as a row indicator and utilizing the next digit as a column indicator, the next result in the table is read off successively until all digits are considered. The last result forms the desired digit of the PIN.

Exemplary embodiments of the present invention are represented by several figures in the drawing and are elucidated in the following description. The figures show:

Figure 1 a diagram for generating a customer-specific binary code;

Figure 2 a diagram for generating a PIN through conversion to a decimal number;

Figure 3 a diagram for generating a PIN by a digit-by-digit conversion into decimal numbers;

Figure 4 a diagram for generating a PIN by a digit-by-digit conversion, including modulus formation; and

Figure 5 a diagram for generating a PIN by reducing hexadecimal numbers with the assistance of mathematical groups.

Identical or corresponding parts are provided with the same reference numerals in the figures.

Figure 1 depicts a flow diagram for converting personal data Dc of a customer using a secret key K into a binary number B of L bits length. The binary number B is part of the 64-bit long encryption result, which was generated from the customer data Dc using the DES algorithm.

If the length of the binary number B equals 13, and if the number of the PIN digits to be generated equals 4, then the PIN, as shown in Figure 2, can be generated by interpreting the binary number B as decimal number D by adding a constant C thereto. The constant is to be selected such that the PIN does not have any leading zeros. In this manner, 8192 different PINS can be generated, which are absolutely uniformly distributed over the number domain in question.

Figure 3 depicts how a binary number of length 13 can be converted into a PIN in that for each digit of the PIN to be generated, a number of bits of the binary number is converted into a decimal number, and a constant C is added to the resultant number D, to avoid having leading zeros of the PIN.

In this manner, 7777 different PINS may be generated, which are absolutely uniformly distributed over the number domain in question.

Another possibility for generating nearly equally distributed PINs from a binary number B is illustrated in Figure 4. The binary number B has 52 digit positions. To generate the four-digit PIN, the binary number B is subdivided into four subsets, which, in the example, have the same length. Each of these subsets is interpreted as a decimal number. The first digit of the PIN is derived as a remainder of a division of the first decimal number by 9. The following digits of the PIN are derived in each case as a remainder of a division of the following decimal number by 10. In this manner, 9000 different PINS may be generated, which are absolutely uniformly distributed.

From the personal data Dc of a customer, as shown in Figure 5, a sequence of 210 hexadecimal digits is generated with the assistance of a secret key and a random-number generator, in that, for example, an encryption result of the DES algorithm from Figure 1 is again encrypted using the algorithm, and so forth. The 14 64-digit binary codes resulting therefrom are converted into 14 hexadecimal numbers Hi, each having 16 digits. Lined up, this yields 224 hexadecimal digits, of which 210 enter into the generation of the PIN.

There are 210 different possibilities fi for mapping the set of 16 hexadecimal digits into the set of the 10 decimal digits. Therefore, each of the 210 hexadecimal digits is converted using a different one of these mappings into a decimal digit di. In order to produce a digit Zi of a PIN from the 210 decimal digits, they are successively linked using the group operation F of any arbitrary ten-element mathematical group; the last result is the sought after digit. Thus, the previously non-uniform, statistical distribution of the 210

decimal digits is evened out. The entire process is repeated for each of the digit positions Z2 through Z4 of the PIN.

Analogously for the first digit of the PIN, 36 hexadecimal digits are generated, which are mapped with every other one of the 36 possible mappings of the hexadecimal digits into the set of the digits 1 through 9, into a digit between 1 and 9. The 36 decimal digits are linked to the first digit of the PIN using the group operation of any arbitrary mathematical group of the order 9. This enables 9000 different PINs to be generated which are nearly uniformly distributed. In generating 10^5 PINs, the maximum non-uniformities amounted to about 1.5 percent. This does not significantly raise the probability of a PIN being accidentally correctly guessed as compared to the theoretical minimum value. Thus, the method functions very reliably.

All mathematical groups having ten elements are fundamentally suited for use with this method. Known representatives include the additive group of the integers modulo 10, $Z_{10,+}$, the multiplicative group of the integers modulo 11, Z^*_{11}, as well as the group of the symmetric mappings of a regular pentagon D5, the so-called dihedral group. In the last instance, one decimal digit, which may be used for the calculation, is assigned to each of the individual elements of the group.

What is claimed is:

1. A method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual, wherein the PINs are generated such that they are randomly uniformly distributed over the available number domain.

2. The method as recited in Claim 1,
wherein the first n1 digits of the binary number (B) are converted in generally known fashion into a decimal number d1, the predefinable natural number n1 being selected so as to yield a natural number z1 such that the quotient $2^{n1}/(z1*9)$ is close to 1; and the first decimal digit of the PIN receives the value d1 modulo 9; N-1 further groups of further n2 digits of the binary number (B) are converted each time in generally known fashion into N-1 decimal numbers d2 through dN, the predefinable number n2 being selected so as to yield a natural number z2 such that the quotient $2^{n2}/(Z2*10)$ is close to 1, to satisfy the condition: $0<=2^{n2}$ modulo $10<3$, and the decimal digits 2 through N of the PIN receive the values di modulo 10, i=2 through N.

3. The method as recited in Claim 2,
wherein n1 and n2<=16 are predefined.

4. The method as recited in one of the preceding claims, wherein N=4 is selected.

5. The method as recited in one of the preceding claims, wherein the binary number (B) has the length L=16, N=4 is predefined, and n1=n2=4 are predefined.

6. The method as recited in Claim 1,
wherein the binary number (B) has the length L=3*n3, n3 groups of three digits of the binary number (B) are converted in generally known fashion into n3 decimal digits to generate the n3 digits of the PIN, n3 being a natural number.

7. The method as recited in Claim 1,
wherein the binary number (B) is fully converted, in generally known fashion, into a decimal number in order to generate the PIN, and, if necessary, a correction value of such kind is added to the resultant decimal number that the first digit of the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.

8. The method as recited in Claim 7,
wherein the binary number (B) has a length L of 13, the generated decimal number has four digits, and a preset value greater than 999 and smaller than 1807 is added to the decimal number.

9. The method as recited in Claim 8,
wherein the set of numbers 0 through 8191 is allocated to n5 subsets Ml,...,Mn5, and a preset value di is added to the generated decimal number if it is an element of the set Mi, it holding that 999<dl<d2<...<dn5<1809, and n5 being a natural number.

10. The method as recited in Claim 7,
wherein the binary number (B) has a length L of 16, the generated decimal number has five digits, and a preset value greater than 9999 and smaller than 34465 is added to the decimal number.

11. The method as recited in Claim 10,
wherein the set of numbers 0 through 65535 is allocated to n5 subsets Ml,...,Mn5, and a preset value di is added to the generated decimal number if it is an element of the set Mi, it holding that 9999<dl<d2<...<dn5<34465, and n5 being a natural number.

12. The method as recited in Claim 1,
wherein to generate the first digits of the PIN, the following steps are executed:

- a pseudo-random number composed of up to 36 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted using one different one out of the 36 possible different mathematical mappings of hexadecimal digits into the digits 1 through 9, into a digit of the digits 1 through 9;
- to even out the probability of the particular PIN digit occurring, the up to 36 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit unequal to zero, which represents the first digit of the PIN;

and the following steps are executed for the second and each following digit of the PIN to be generated:

- a pseudo-random number composed of up to 210 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted into one decimal digit using each time one different one out

of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;

- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN.

13. The method as recited in Claim 12,
wherein the first digit of the PIN is generated in that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and the second and the following digits of the PIN are generated, in that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.

14. The method as recited in Claim 13,
wherein the additive group of the integers modulo 10 are used to link the up to 210 digits.

15. The method as recited in Claim 13,
wherein the multiplicative group of the integers modulo 11 are used to link the up to 210 digits.

16. The method as recited in Claim 13,
wherein the group of the symmetric mappings of a regular pentagon (dihedral group) is used to link the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit.

17. The method as recited in Claim 16,
wherein the digit 0 is assigned to the identity mapping, the digits 1 through 4 to the four rotations about the midpoint of the pentagon, and the digits 5 through 9 to the five reflections about the five axes of symmetry of the pentagon.

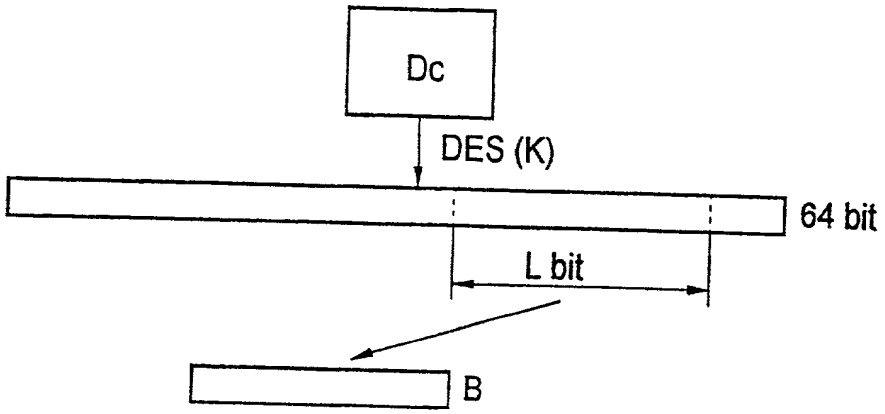

Fig.1

L = 13,
N = 4,
PINmax-PINmin=8192

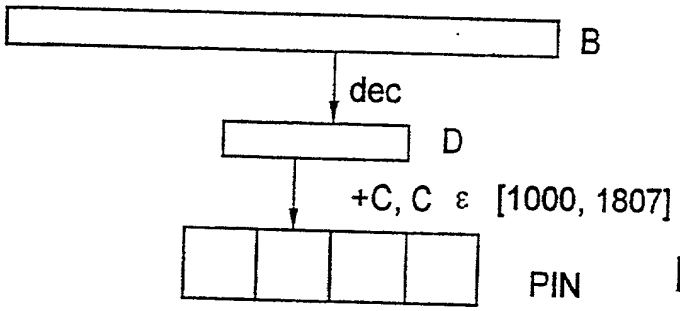

Fig.2

L = 12,
N = 4,
PINmax-PINmin=7777

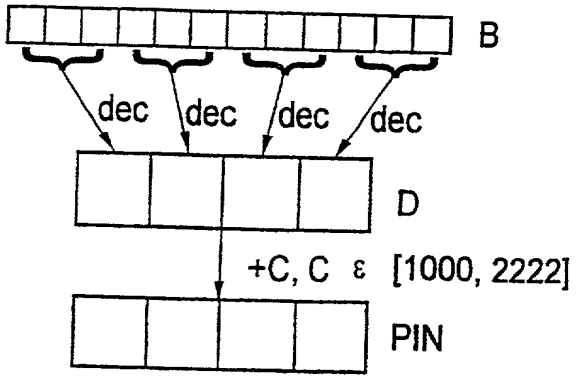

Fig.3

L = 52,
N = 4,
PINmax-PINmin=9000

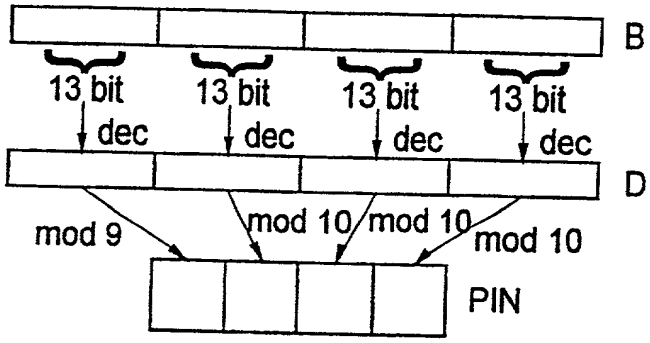

Fig.4

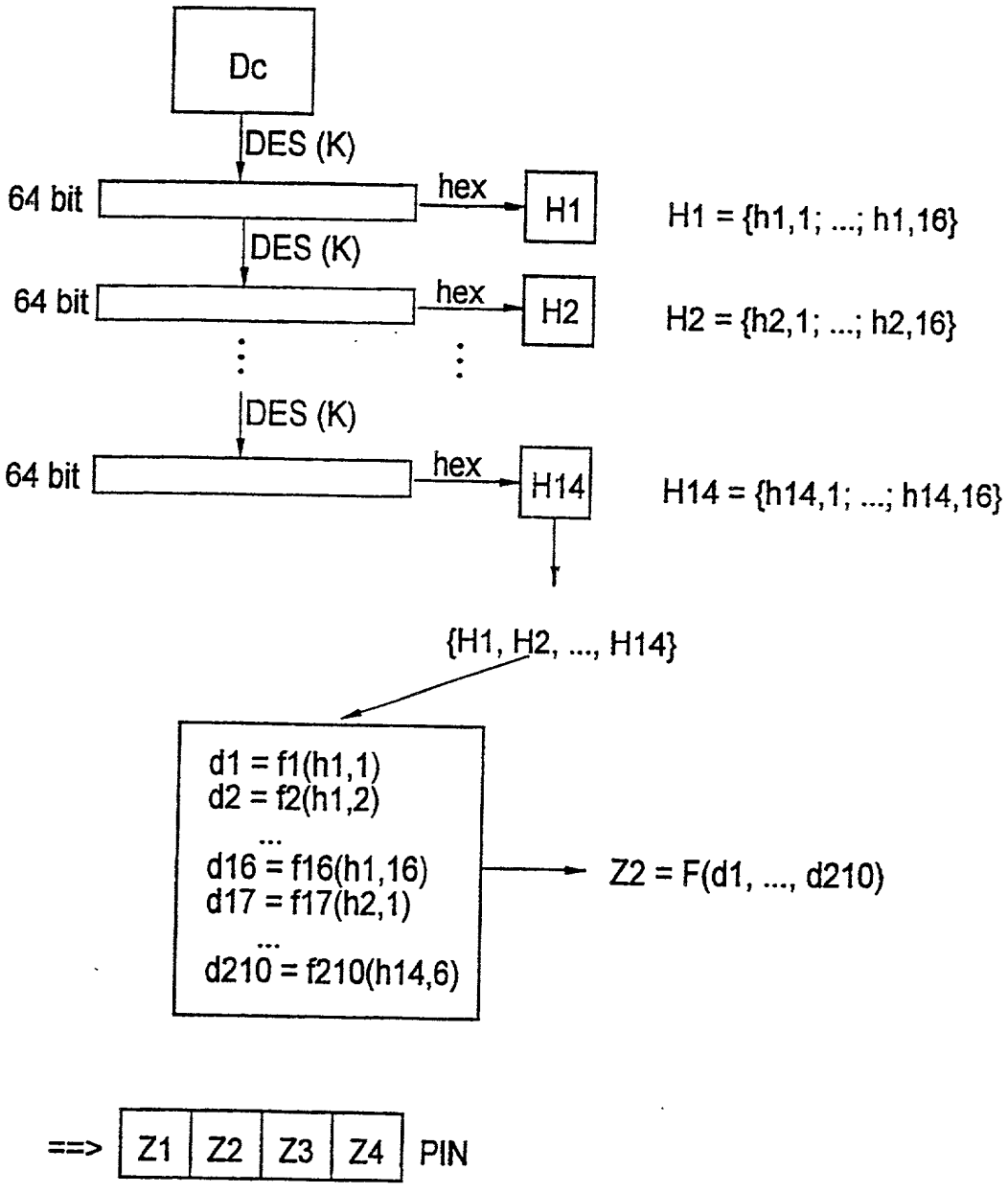
Dc
DES (K)
64 bit
hex
H1
H1 = {h1,1; ...; h1,16}
DES (K)
64 bit
hex
H2
H2 = {h2,1; ...; h2,16}
DES (K)
64 bit
hex
H14
H14 = {h14,1; ...; h14,16}
{H1, H2, ..., H14}
d1 = f1(h1,1)
d2 = f2(h1,2)
...
d16 = f16(h1,16)
d17 = f17(h2,1)
...
d210 = f210(h14,6)
Z2 = F(d1, ..., d210)
==>
Z1
Z2
Z3
Z4
PIN

Fig.5

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR GENERATING IDENTIFICATION NUMBERS**, the specification of which was filed as International Application No. PCT/EP00/02481 on March 21, 2000 and filed as an application for Letters Patent in the U.S.P.T.O. on October 1, 2001.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
199 14 407.9	Fed. Rep. of Germany	March 30, 1999	Yes

Express Mail No. EL430986254US

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004

CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Joerg SCHWENK**

Inventor's Signature: Jörg Schwenk

Date: 23.11.01

Residence: ~~Suedwestring 27~~ Weissh. 10
D-~~64807 Dieburg~~ 91239 Henfeld DEY
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.

Inventor: **Tobias MARTIN**

Inventor's Signature: Tobias Martin

Date: 21/11/2009

Residence: Spitzengaerten 1
D-35466 Rabenau-Ruddinghausen DE
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR GENERATING IDENTIFICATION NUMBERS**, the specification of which was filed as International Application No. PCT/EP00/02481 on March 21, 2000.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
199 14 407.9	Fed. Rep. of Germany	March 30, 1999	Yes

Express Mail No. EL244508211US

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004

CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Joerg SCHWENK**

Inventor's Signature: _____

Date: _____

Residence: Suedwestring 27
D-64807 Dieburg
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.

Inventor: **Tobias MARTIN**

Inventor's Signature: _____

Date: _____

Residence: Spitzengaerten 1
D-35466 Rabenau-Ruddinghausen
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.